E-SAFETY POLICY - UK

VERSION 3.0

Contents

Definitions

- Safeguarding is defined as: protecting children from maltreatment; preventing impairment of children's health or development; ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and taking action to enable all children to have the best outcomes Keeping Children Safe in Education (KCSIE), 2016).
- Child Protection refers to the situation where a child is suffering significant harm, or is likely to do so, and action is required to protect that child.
- 'Children' includes everyone under the age of 18
- DSL: Designated Safeguarding Lead
- DSO: Designated Safeguarding Officer

Rationale & Scope of the Policy

This policy applies to all members of the EC community (including staff, students, volunteers, visitors, partners) who work both inside and outside of EC premises, and sets out how the school discharges its responsibilities relating to safeguarding and promoting the welfare of students at the school. This E-safety policy has links with the wider safeguarding agenda; other relevant policies, external links and procedures are referenced on the last page. This policy will contribute to the safeguarding of pupils/students at EC schools by:

- Providing a clear plan for E-Safety at EC.
- Reducing the potential risks concerned with E-safety.Outlining responsibilities of all staff and specific roles.
- The establishment of a safe, resilient and robust safeguarding ethos in the school, built on mutual respect, and shared values.

Guiding principles

- E-safety is not an IT issue: it is a safeguarding issue
- Though safeguarding protocols and procedures protecting children and vulnerable adults are more stringent then in the past, new risks and challenges are ever present
- EC needs to balance its responsibilities in respect of safeguarding with the need to allow students (especially children) freedom to discover and develop and the ability to learn about risks independently

Relevant Legislation

- Children Act 1989 and 2004
- Counter Terrorism and Security Act 2015
- The Prevent Duty Guidance 2015
- Working Together to Safeguard Children (2015), which sets out the multiagency working arrangements to safeguard and promote the welfare of children and young people and protect them from harm; in addition it sets out the statutory roles and responsibilities of schools.
- Keeping Children Safe in Education (2016) is statutory guidance issued by the Department for Education which all schools and colleges must have regard to when carrying out their duties to safeguard and promote the welfare of children.
- Data Protection Act 1998

Main areas of Risk

The main areas of risk identified are as follows:

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games and film/video material leading to exposure to violence/sexual content/ strong and/or racist language, substance abuse.
- Inappropriate on-line contact with adults / strangers
- Websites promoting for example substance abuse/anorexia/self-harm/suicide
- Hate websites
- Grooming
- Radicalisation
- Cyber-bullying in all forms
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and welfare (amount of time spent online - Internet or gaming)
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright infringement (little care or consideration for intellectual property and ownership – such as music and film)
- Content validation: checking authenticity and accuracy of online content

Policy Statements

EC staff will take all reasonable precautions to ensure E-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on an EC computer or mobile device. EC cannot accept liability for material accessed, or any consequences of Internet access.

1. Whole School Approach

1.1 All policies which address issues of power and potential harm, for example anti-bullying, equal opportunities, handling, positive behaviour, will be linked to ensure a whole school approach.

1.2 The E-safety policy cannot be separated from the general ethos of the school, which should ensure that students are treated with respect and dignity, taught to treat each other with respect, feel safe, have a voice, and are listened to.

1.3 Staff members working with children are advised to maintain an attitude of 'it could happen here' where E-safety is concerned. When concerned about the welfare of a child, staff members should always act in the best interests of the child.

2. Preventing inappropriate content

2.1 All PCs on EC premises and the student Wi-Fi network in centres will be protected by secure firewalls that maintain a barred site list and, as far as possible, prevent anyone accessing inappropriate content online.

3. Data Protection

3.1 Personal data will only be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

3.2 When personal data is stored on any portable computer system, memory stick or any other removable media:

3.2..1 the data will be encrypted and password protected.

3.2.2 the device will be password protected.

3.2.3 the device will offer approved virus and malware checking software.

3.2.4 the data will be securely deleted from the device, in line with EC policy once it has been transferred or its use is complete.

4.Social Media - Protecting Professional Identity

EC has a duty of care to provide a safe learning environment for students and staff. EC could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render EC liable to the injured party.

Reasonable steps to prevent predictable harm must therefore be in place.

EC provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and EC, through limiting access to personal information:

4.1 Staff handbook will include acceptable use.

4.2 Training to include; social media risks.

4.3 Clear reporting guidance will be issued to staff, including responsi bilities, procedures and sanctions.

4.4 EC's use of social media for professional purposes will be checked to ensure compllance with the Social Media, Data Protection, Communications, Digital Image and Video Policies and legislation.

5.Student Support

EC will:

5.1 EC will establish and maintain an ethos where students feel secure and are en couraged to talk, and are listened to.

5.2 Centres will ensure students know that there are people in the school whom they can approach if they are worried or in difficulty

5.3 Offer advice on E-safety as well as advice about what to do if in the event of receiving unwanted contact online or via text, during weekly meetings with students under 18.

5.4 Opportunities will be provided for students to develop skills, con cepts, attitudes and knowledge that promote their E-safety.

5.5 EC has a Code of Conduct for students, that will include advice on E-safety.

6.Prevent

EC understands its responsibilities under the Counter Terrorism & Securities Act 2015 to pre-vent people of all ages being radicalised or drawn into terrorism. EC recognises that E-safety is paramount in this area and seeks to meet its obligations in the ways shown below:

8.1 EC will nominate a person who will liaise with the Centre Directors and other staff about issues to do with protecting students and staff from radicalisation.

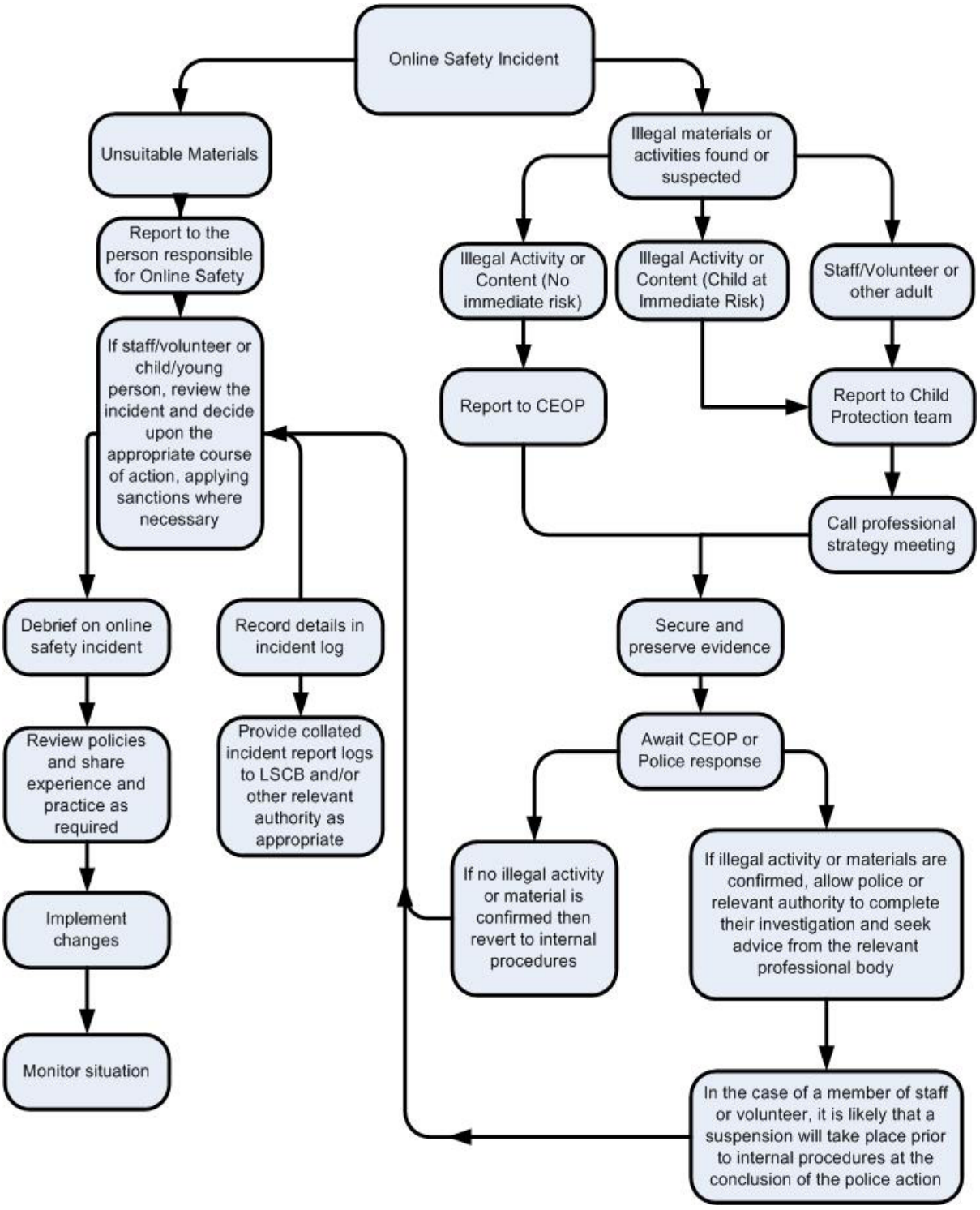
8.2 Responsibility for ensuring the PREVENT policy is carried out lies with the Centre Director and/or Prevent Lead Contact, whose duties are to ensure that the centre and its staff respond to preventing radicalisation on a day-to-day basis, ensure that

7.Responding to incidents of misuse

7.1 Staff and pupils are to be given information about infringements in use and possible sanctions, including:

- Interview/counselling by DOS / Centre Director
- Informing parents or guardians in the case of under 18s
- Removal of Internet or computer access for a period
- Referral to Police / relevant authorities

7.2 If there is any suspicion that web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, staff are to refer to the right hand side of the Flowchart (below) for respond ing to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

8. Training

8.1 All staff members will receive appropriate E-safety training, which is regularly updated. In addition, all staff should receive E-safety updates (for example, via email, e-bulletins and staff meetings), as required, but at least annually, to provide them with relevant skills and knowledge on E-safety.

8.2 Whistle blowing procedures will be covered in whole school training so that staff know what to do if they have concerns relating to E-safety practice within the school.

8.3 All training will be effective and comply with the law at all times.

8.4 The E-safety Coordinator, DSL, and any deputy DSOs, will undergo training to provide them with the knowledge and skills required to carry out their E-safety roles. The training will be updated every two years.

8.5 Online safety training for staff will be integrated, aligned and con sidered as part of the overarching safeguarding approach.

9. Confidentiality and information sharing

9.1 To ensure confidentiality, Information will only be shared appropriately.

9.2 Information about a student will be disclosed to members of staff on a need to know basis only.

10. Communication with parents

10.1 Wherever possible undertake appropriate discussion with parents unless the circumstances preclude this action.

11. Record Keeping

EC will:

11.1 Keep clear detailed written records of concerns about E-safety (noting the date, event and action taken), even where there is no need to refer the matter to local authorities immediately.

11.2 Ensure all records are kept securely.

Roles and Responsibilities

The following section outlines the roles and responsibilities of all EC staff together with role specific responsibilities in relation to this policy.

All staff

All staff should be made aware of their responsibility to maintain confidentially and aware of their duties to report and record any E-safety concerns they may have in accordance with centre E-safety, safeguarding and child protection procedures.

All staff need to be aware of the systems within EC which support E-safety, safeguarding and child protection – this forms part of the induction process but also on-going training which is regularly updated.

All staff will:

- Read, understand and help promote EC's E-safety policies and guidance.
- Understand and adhere to EC's Acceptable Use Policy.
- Be aware of E-safety issues related to the use of mobile phones, cameras and hand held devices and monitor their use and implement current EC policies with regard to these devices.
- Report any suspected misuse or problem to the E-safety coordinator/DSL.
- Maintain an awareness of current E-safety issues and guidance e.g. through CPD.
- Model safe, responsible and professional behaviours in their own use of technology.
- Ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
- At all times take care to ensure the safe keeping of student/staff personal data, minimizing the risk of its loss or misuse.
- Use student/staff personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using student/staff personal data.
- Transfer student/staff personal data using encryption and secure password protected devices only.
- Adhere to standards listed above when staff/student personal data is stored on any portable computer system.
- Not engage in online discussion on personal matters relating to members of the EC community
- Not attributed any personal opinions posted online to EC
- Ensure security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Operational Leadership

The Operational leadership is responsible for the approval of and reviewing the effectiveness of this policy. This will be carried out through the receiving of regular information regarding E-safety incidents and monitoring reports.

The Operational leadership will ensure that:

- EC has an E-safety policy in accordance with relevant legislation and this is reviewed annually.
- EC operates, "safer recruitment" procedures and ensures that appropriate checks are carried out on all new staff and relevant volunteers.
- A member of each centre's senior leadership team is appointed as the E-safety Coordinator.
- E-safety Coordinators attend appropriate refresher training every two years.
- Centres remedy any deficiencies or weaknesses brought to their attention without delay.
- Centres have procedures for dealing with allegations/issues of E-safety or misuse.
- A member of the Operational Leadership is appointed with a specific brief for safeguarding and child protection and E-safety, and will liaise with the Centre Directors and DSLs. The role is s trategic rather than operational – they will not be involved in concerns about individual pupils/students.
- The member of the Operational Leadership nominated to be responsible for safeguarding will be responsible for liaising with the local authority and other partner agencies in the event of allegations of abuse being made against the Centre Director.

Centre Director

Each EC Centre Director has a duty of care to ensure the safety (including E-safety) of members of the school community, though the day to day responsibility for E-safety may be delegated to the E-safety Co-ordinator / DSL.

The Centre Director will:

- Take overall responsibility for E-safety provision in the centre
- Take overall responsibility for data and data security in the centre
- Ensure the centre uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. KCSIE
- Be responsible for ensuring that staff receive suitable training to carry out their E-safety roles and to train other colleagues, as relevant
- There is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role. This is to provide a safety net and also support those staff members who take on important monitoring roles
- Hold regular reviews with the E-safety Co-ordinator / DSL including:
    - o E-safety incident logs
    - o filtering / change control logs
- The Centre Director and (at least) another member of staff are aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff. (see flow chart on dealing with E-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures)

E-safety Coordinator

Each EC centre will have a named member of staff with day to day responsibility for E-safety. Centres may choose to combine this with the Designated Safeguarding Officer (DSO) / Designated Safeguarding Lead (DSL) role.
Where possible, centres will appoint a staff member with a child welfare background, preferably with good knowledge and understanding of new technologies.

Each E-safety Coordinator / DSL will:

- Take day to day responsibility for E-safety issues and have a leading role in establishing and reviewingthe school E-safety procedures
- Ensure that all centre staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place
- Provide training and advice for staff
- Liaise with the Local Authority / relevant body
- Liaise with EC technical staff
- Receive reports of E-safety incidents and create a log of incidents to inform future E-safetydevelopments
- Attend relevant meetings
- Report regularly to the Centre Director on E-safety issues

DSL/DSO

EC recognises that technology provides additional means for child protection issues to develop.
The DSLs/DSO will:

- Be trained in E-safety issues and be aware of the potential for serious child protection / safeguardingissues to arise from the risk areas listed above.
- Liaise with the Centre Director and E-safety Coordinator over E-safety matters in the school

Network Manager / IT staff

The Network Manager / IT Staff will ensure:

- That EC's technical infrastructure is secure with 3 layers of anti-virus: on desktops, on perimeterconnections and on email.
- That all data held on pupils on the school office machines have appropriate access controls in placewith structured permission on the company SharePoint and restricted shared folders at local level.
- That provision exists for intrusion detection and malicious attack detection (e.g. keeping virusprotection up to date)
- That access controls / encryption exist to protect personal and sensitive information held on school-owned devices
- That the use of the network / internet / Virtual Learning Environment / remote access / email is loggedin order that any misuse / attempted misuse can be recorded.
- That appropriate backup procedures exist so that critical information and systems can be recovered inthe event of a disaster
- Relevant IT staff keep up to date with the school's E-safety policy and technical information

Homestay Hosts

Homestay hosts will:

- Know the names of the DSL and DSO at their centre and how to contact them.
- Support EC in promoting good practice and endorse the E-safety Policy – UK.
- Liaise with the centre DSL/DSO on E-safety issues and the welfare

Related documents:	• UK Staff handbook • Whistleblowing • Code of Conduct for staffRelated
Related SOPs:	
Related Policies:	• Anti-Bullying policy • Safeguarding & Child Protection Policy - UKExternal
External Links:	• NSPCC E-safety portal: Link • Professionals Online Safety helpline: • www.saferinternet.org.uk/about/helpline